

La Biblioteca di Atlantide
Quaderni di letteratura grigia

(CC) 2005. Quest'opera è stata rilasciata sotto la licenza
Creative Commons Attribuzione - Non commerciale - Non opere derivate.

Per leggere una copia della licenza visita il sito web

<http://creativecommons.org/licenses/publicdomain/>

o spedisce una lettera a

Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA.

www.sergiofumich.com

Ca' "La Gatera"

26822 Brembio (LO) – Via Togliatti, 3

Sergio Fumich

I NUMERI NATURALI

APPUNTI DI MATEMATICA ELEMENTARE
DAL PUNTO DI VISTA SUPERIORE

Ca' "La Gatera"

2005

PREMESSE INSIEMISTICHE

Gli *insiemi* e gli *elementi* che li costituiscono si indicano solitamente con le lettere dell'alfabeto latino (gli insiemi con le lettere maiuscole, gli elementi con le lettere minuscole). Talvolta si usa anche il termine *punto* per indicare l'elemento di un insieme.

Le frasi " x appartiene ad un insieme E " oppure " x è un elemento di E " o " x è un punto di E " hanno tutte lo stesso significato e si rappresentano simbolicamente con $x \in E$. Il simbolo $\in$ è il simbolo di *appartenenza*. La negazione di questo simbolo si rappresenta con il simbolo $\notin$ e la frase " x non appartiene ad E " si rappresenta con $x \notin E$.

Si dice che un insieme E è contenuto in un insieme F se ogni elemento x di E è elemento di F . Tale proprietà si indica simbolicamente con $E \subset F$. La frase " F contiene E " ha lo stesso significato di " E è contenuto in F " e si indica con $F \supset E$. I simboli $\subset, \supset$ sono i simboli di *inclusione*.

Quando è contemporaneamente $E \subset F$ e $F \subset E$, si dice che " E è uguale a F " o che " E coincide con F " e si scrive $E = F$. Questa uguaglianza significa che ogni elemento di uno qualunque dei due insiemi appartiene all'altro. La sua negazione si indica con $E \neq F$ ed indica che esiste un elemento di uno dei due insiemi che non appartiene all'altro.

Il simbolo $\Rightarrow$ indica la *conseguenza logica*. Se P e Q indicano proprietà relative agli elementi di un insieme, la

scrittura $P \Rightarrow Q$ significa che la proprietà P *implica* la proprietà Q , cioè che Q è vera ogni volta che lo è P .

Se si verifica anche la proprietà reciproca, cioè se ogni volta che Q è vera lo è anche P , si scrive $P \Leftrightarrow Q$. Il simbolo $\Leftrightarrow$ è il simbolo dell'*equivalenza logica* e lo si esprime con "*è necessario e sufficiente*". La scrittura $P \Leftrightarrow Q$ si legge "*condizione necessaria e sufficiente perché P sia vera è che lo sia Q* ".

Il simbolo $\forall$ si legge "*per ogni*" o "*qualsiasi*". È il *quantificatore universale*. Il simbolo $\exists$ si legge "*esiste*". È il *quantificatore esistenziale*.

Sia E un insieme. Si dice che A è una *parte* di E o un *sottoinsieme* di E se $A \subset E$. Se una parte di E ha il solo elemento a , essa si indica con $\{a\}$.

La parte di E che non contiene alcun elemento si indica con $\emptyset$ e si chiama la *parte vuota* di E . È definita ad esempio da $\{a: a \in E \text{ e } a \neq a\}$.

L'*intersezione* di due insiemi A e B è l'insieme degli elementi appartenenti tanto ad A quanto a B . La si indica con $A \cap B$. È:

$$a \in A \text{ e } a \in B \Leftrightarrow a \in A \cap B$$

Se $A \cap B = \emptyset$, A e B si dicono *disgiunti*.

L'*unione* di due insiemi A e B è l'insieme degli elementi che appartengono ad A o a B . La si indica con $A \cup B$. È:

$$a \in A \text{ o } a \in B \Leftrightarrow a \in A \cup B$$

Sia E un insieme ed A una parte di E . L'insieme degli elementi di E che non appartengono ad A si chiama il *complementare* di A relativo ad E . Lo si indica con ${}_{CE}A$. È:

$$a \in E \text{ e } a \notin A \Leftrightarrow a \in {}_{CE}A$$

È:

$$A \cup {}_{CE}A = E, A \cap {}_{CE}A = \emptyset$$

Siano E e F due insiemi distinti o non distinti. Si chiama *prodotto* di E per F l'insieme costituito da tutti gli elementi ottenuti prendendo le coppie di due elementi, il primo, x , appartenente ad E , il secondo, y , appartenente a F . Il prodotto di E per F si indica con $E \times F$, ed un elemento di tale prodotto si indica con (x, y) dove $x \in E$, $y \in F$. In generale, $E \times F$ e $F \times E$ sono insiemi distinti. Se $E = F$, si scrive anche E^2 invece di $E \times E$.

Dati un insieme E ed un insieme F , ogni legge f che associa ad ogni elemento di E un ben determinato elemento di F , è detta una *applicazione* di E in F . Se x è un elemento di E , l'elemento di F che la f associa ad x si indica con $f(x)$. Si dice che $f(x)$ è l'immagine di x tramite la f . E ed F si dicono *dominio* e *codominio* della f .

Sia E un insieme, A una parte di $E \times E$; si dice che due elementi x, y di E sono legati da una *relazione binaria* definita da A se $(x, y) \in A$. Solitamente si usa una notazione più comoda che mette in evidenza il fatto che i due elementi sono legati da una relazione binaria; in generale, se con R si indica la relazione, si scriverà xRy .

Una relazione si dice *riflessiva* se xRx è vera per ogni $x \in E$; *simmetrica* se $xRy \Leftrightarrow yRx$; *transitiva* se xRy e $yRz \Rightarrow xRz$; *antisimmetrica* se xRy e $yRx \Rightarrow x=y$.

Una relazione è una *relazione di equivalenza* se è riflessiva, simmetrica e transitiva. Una relazione è una *relazione d'ordine* se è riflessiva, antisimmetrica e transitiva.

I NUMERI NATURALI

I numeri **0, 1, 2, 3, 4, 5, 6, 7, ...**, si chiamano *numeri naturali*. Con **N** si indicherà il loro insieme, mentre con **N⁺** sarà indicato l'insieme $\mathbb{N}\{0\}$.

La costruzione dell'insieme **N** è basata su alcune proprietà di **N**, note come *assiomi di Peano*:

(A1) Zero è un numero naturale.

(A2) A ogni numero naturale **n** corrisponde un altro numero naturale, univocamente determinato, che si chiama *successivo* di **n** e si indica con **n⁺**.

(A3) Il successivo di un numero naturale non è mai zero.

(A4) Se due numeri naturali hanno lo stesso successivo, sono uguali.

(A5) Sia **A** una parte di **N** che contenga lo zero e tale che, se **A** contiene **n**, **A** contiene anche il suo successivo **n⁺**. **A** coincide allora con l'insieme **N** di tutti i numeri naturali (Assioma d'induzione o di ricorrenza).

L'assioma (A1) definisce un numero naturale: lo zero. L'insieme **N** non è vuoto. Partendo da tale numero si costruiscono tutti gli altri.

L'assioma (A2) introduce una corrispondenza che dà il procedimento generale di costruzione dell'insieme dei numeri naturali: $x \rightarrow x^+$.

L'assioma (A3) impedisce che si ritorni allo zero, impedisce cioè: $0 \rightarrow 0^+ \rightarrow 0$. L'insieme $\{0, 0^+\}$ non verifica (A3).

L'assioma (A4) impedisce la ricomparsa nella catena $\dots x_i \rightarrow x_i^+ \dots$ di uno stesso numero. L'applicazione $x \rightarrow x^+$ è biunivoca su $\mathbf{N}^+$; pertanto, ogni numero naturale diverso da 0 è il successivo di un altro naturale, il quale è unico e si chiama il *precedente* di x . Applicando, dunque, la corrispondenza $x \rightarrow x^+$ all'ultimo numero ottenuto in una tappa della costruzione, se ne ottiene uno nuovo, distinto da tutti quelli già ottenuti, sul quale si può ricominciare l'operazione. La catena è illimitata. Si dice che $\mathbf{N}$ è un insieme *infinito*.

L'assioma (A5) permette di concepire l'insieme $\mathbf{N}$ nella sua completezza. L'assioma (A5) può essere così interpretato:

Sia $\mathbf{A}$ l'insieme dei numeri naturali per i quali sia vera una proprietà $\mathbf{P}$. Supponiamo che siano vere le proposizioni " $\mathbf{P}$ è vera per zero" e "se $\mathbf{P}$ è vera per x allora $\mathbf{P}$ è vera per x^+ ". Si può per l'assioma (A5) affermare che " $\mathbf{P}$ è vera per tutti i numeri naturali".

Concludendo: i primi quattro assiomi determinano la costruzione di $\mathbf{N}$; il quinto fornisce uno strumento logico per il ragionamento in questo insieme.

Costruito l'insieme dei numeri naturali, bisogna dargli una struttura. Cominciamo col definire l'operazione di addizione.

Facciamo corrispondere ad ogni coppia ordinata (x, y) di numeri naturali un numero naturale detto *somma*

di x e y ed indicato con $x+y$ definito per ricorrenza come segue:

- a) $x+0 = x$
- b) supposto definito $x+y$, definiamo $x+y^+$ mediante la $x+y^+ = (x+y)^+$.

L'operazione è definita prima per $y=0$; cerchiamo l'insieme A degli y per i quali l'operazione è definita. È $0 \in A$. Se l'addizione è definita per y , la proposizione b) definisce l'addizione per y^+ . Supposto di aver ottenuto $x+y$, il numero $x+y^+$ è allora il successivo di $x+y$; pertanto se $y \in A$ allora $y^+ \in A$, e dunque per l'assioma (A5) è $A=N$.

L'addizione dello zero non ha effetto alcuno su x . Poniamo $1=0^+$. Si ha: $x+0^+=(x+0)^+$, cioè $x+1=x^+$.

Dimostriamo che per x, y, z numeri naturali qualsiasi si ha:

$$(x+y)+z=x+(y+z) \quad [\text{proprietà associativa}].$$

Si supponga che x, y siano fissati. Dimostriamo la relazione per $z=0$. Per definizione si ha: $(x+y)+0=x+y$ e $x+(y+0)=x+y$, dunque la relazione è vera per $z=0$. Supponiamo ora che sia dimostrata per z e dimostriamola per z^+ , cioè dimostriamo $(x+y)+z^+=x+(y+z^+)$.

È: $(x+y)+z^+=[(x+y)+z]^+=[x+(y+z)]^+=x+(y+z)^+=x+(y+z^+)$. Pertanto per l'assioma (A5) è vera per uno z qualsiasi.

Invece di scrivere $(x+y)+z$ oppure $x+(y+z)$ si può scrivere $x+y+z$.

Dimostriamo che per x, y numeri naturali qualsiasi si ha:

$$x+y=y+x \quad [\text{proprietà commutativa}].$$

Proviamo da prima che $x+0=0+x$, cioè che è vera per $y=0$. Per la definizione di somma è $x+0=x$, proviamo che anche $0+x=x$. La proprietà è vera per $x=0$ perché $0+0=0$. Supponiamo di averla dimostrata per x , dimostriamola per x^+ . Si ha: $0+x^+=(0+x)^+=x^+$. Dunque è vera per qualunque x .

Proviamola per $y=1$, cioè proviamo che $x+1=1+x$. È vera per 0 . Supponiamo che sia vera per x e mostriamo che è vera per x^+ . È:

$$x^++1=(x+1)+1=(1+x)+1=1+(x+1)=1+x^+.$$

È dunque vera per un x qualsiasi.

Dimostriamo ora che, supposta vera per y qualunque, è vera per y^+ :

$$\begin{aligned} x+y^+ &= x+(y+1) = (x+y)+1 = (y+x)+1 = y+(x+1) = y+(1+x) = \\ &= (y+1)+x = y^++x. \end{aligned}$$

Dunque è vera per qualunque coppia (x, y) di naturali.

Dimostriamo che se a, b sono due numeri naturali tali che $a+b=0$, allora $a=b=0$.

Se $b \neq 0$, esiste b' tale che $b'+1=b$ e pertanto $a+b=0 \Rightarrow a+b'+1=(a+b')^+=0$, che contrasta con l'assioma (A3). Pertanto $b=0$, e di conseguenza $a=0$.

Dimostriamo che per x qualsiasi:

$$a+x=b+x \Rightarrow a=b.$$

Per $x=0$ è evidente.

Supponiamo dimostrato $a+x=b+x \Rightarrow a=b$ e dimostriamo che $a+x^+=b+x^+ \Rightarrow a=b$. È:

$$\mathbf{a+x^+=b+x^+ \Rightarrow (a+x)^+=(b+x)^+ \Rightarrow {}^*a+x=b+x \Rightarrow a=b.}$$

Pertanto l'implicazione è vera qualunque sia $\mathbf{x}$.

Tale proprietà si chiama *proprietà della semplificazione dell'addizione*. Ogni naturale è *semplificabile* o *regolare* per l'addizione.

* Per l'assioma (A4).

LA RELAZIONE D'ORDINE TOTALE IN $\mathbf{N}$

Dati due numeri naturali $\mathbf{a}$, $\mathbf{b}$, se esiste un numero naturale $\mathbf{x}$ tale che $\mathbf{a}+\mathbf{x}=\mathbf{b}$, si dice che $\mathbf{a}$ è *minore o uguale a* $\mathbf{b}$ e si scrive $\mathbf{a}\leq\mathbf{b}$, oppure che $\mathbf{b}$ è *maggiore o uguale ad* $\mathbf{a}$ e si scrive $\mathbf{b}\geq\mathbf{a}$. Il numero $\mathbf{x}$ si chiama *differenza* di $\mathbf{a}$ e $\mathbf{b}$ e si indica con $\mathbf{x}=\mathbf{b}-\mathbf{a}$.

La definizione introduce una relazione in $\mathbf{N}$:

$$\mathbf{a}\leq\mathbf{b} \Leftrightarrow \exists \mathbf{x}: \mathbf{a}+\mathbf{x}=\mathbf{b}.$$

Il problema "*Esiste un numero naturale x tale che $a+x=b$?*" si chiama *equazione*. Rispondere a questa domanda significa *risolvere* l'equazione. Ogni numero naturale che risponde alla domanda si chiama *soluzione*.

(*Unicità della soluzione*). Se esiste $\mathbf{x}$, esso è unico. Infatti, se esistesse un altro $\mathbf{x}'$ si avrebbe $\mathbf{a}+\mathbf{x}=\mathbf{a}+\mathbf{x}'$ da cui $\mathbf{x}=\mathbf{x}'$.

Consideriamo due casi particolari:

($\mathbf{a}=\mathbf{b}$). È $\mathbf{a}+\mathbf{x}=\mathbf{a}$ che si può scrivere $\mathbf{a}+\mathbf{x}=\mathbf{a}+\mathbf{0}$, da cui $\mathbf{x}=\mathbf{0}$. Ne consegue che per ogni naturale $\mathbf{a}$ è $\mathbf{a}\leq\mathbf{a}$, cioè la relazione $\leq$ è riflessiva.

($\mathbf{a}=\mathbf{0}$). È $\mathbf{0}+\mathbf{x}=\mathbf{b}$, cioè $\mathbf{x}=\mathbf{b}$. Ne consegue che per ogni naturale $\mathbf{b}$ è $\mathbf{b}\geq\mathbf{0}$.

Non sempre esiste la soluzione. Ad esempio, $\mathbf{1}+\mathbf{x}=\mathbf{0}$: l'assioma (A3) ci assicura che non esiste un numero naturale x che risolva l'equazione.

Dimostriamo che:

$$a \leq b \text{ e } b \leq a \Leftrightarrow a = b \quad (\text{proprietà antisimmetrica}).$$

Si sa già che la relazione è riflessiva, pertanto è:
 $a = b \Rightarrow a \leq b \text{ e } b \leq a$.

Dimostriamo ora che $a \leq b \text{ e } b \leq a \Rightarrow a = b$. È:

$$a \leq b \Rightarrow \exists c: a + c = b, \quad b \leq a \Rightarrow \exists d: b + d = a;$$

ne segue:

$$a + c = b \Rightarrow (a + c) + d = b + d \Rightarrow a + c + d = a \Rightarrow c + d = 0 \Rightarrow c = d = 0.$$

Dimostriamo che:

$$a \leq b \text{ e } b \leq c \Rightarrow a \leq c \quad (\text{proprietà transitiva}).$$

È: $a \leq b \Rightarrow \exists d: a + d = b, \quad b \leq c \Rightarrow \exists e: b + e = c$; si ha:

$$a + d = b \Rightarrow a + d + e = b + e \Rightarrow a + d + e = c \Rightarrow a \leq c.$$

La relazione $\leq$ è una relazione d'ordine totale, cioè: $\forall a, b \quad a \leq b \text{ o } b \leq a$.

Lo dimostreremo fissando b . Sia A l'insieme dei numeri naturali per i quali è verificata una delle due relazioni: $a \leq b \text{ o } b \leq a$. Dimostriamo che $0 \in A$: infatti per b qualsiasi è $0 \leq b$. Dimostriamo che $a \in A \Rightarrow a^+ \in A$. L'ipotesi di ricorrenza implica uno o l'altro dei due casi $a \leq b$ oppure $b \leq a$. Se $b \leq a$, $\exists c: b + c = a$ da cui $b + c + 1 = a + 1$ e quindi $b \leq a^+$. Dunque, $a^+ \in A$. Se $a \leq b$, supponiamo $a \neq b$ in quanto il caso $a = b$ è compreso nel caso precedente. Esiste allora $c \neq 0$ tale che $a + c = b$. Essendo $c \neq 0$, esso ha un precedente c' , cioè $\exists c': c' + 1 = c$ per cui è:

$$a + c = a + c' + 1 = (a + 1) + c' = b,$$

quindi $a^+ \leq b$ cioè $a^+ \in A$.

In definitiva per (A5) è $A=N$.

La differenza $b-a$ non cambia aggiungendo ai due termini uno stesso numero c .

È: $x=b-a \Leftrightarrow a+x=b$, di conseguenza $(a+c)+x=b+c$, cioè $x=(b+c)-(a+c)$.

Dimostriamo che:

$$a \leq b \text{ se e solo se } a+c \leq b+c.$$

La $a \leq b \Rightarrow a+c \leq b+c$ discende dalla precedente asserzione. Il viceversa sia ha da: $(a+c)+x=b+c \Rightarrow a+x=b$.

Le disuguaglianze $a \leq b$ e $c \leq d$ possono essere sommate membro a membro, cioè:

$$a \leq b \text{ e } c \leq d \Rightarrow a+c \leq b+d.$$

È: $a \leq b \Rightarrow a+c \leq b+c$, $c \leq d \Rightarrow b+c \leq b+d$, per la transitività è: $a+c \leq b+d$.

(Relazione d'ordine stretto). Se esiste un $x \neq 0$ tale che $a+x=b$, si dice che " a è minore di b " e si scrive $a < b$ oppure che " b è maggiore di a " e si scrive $b > a$.

Se $a < b$, la differenza $b-a$ esiste e non è zero.

La relazione d'ordine stretto è transitiva, cioè è:

$$a < b \text{ e } b < c \Rightarrow a < c.$$

È inoltre:

$$a < b \Rightarrow a+c < b+c$$

$$a < b \text{ e } c < d \Rightarrow a+c < b+d.$$

Sia $a \leq b$. Si dice *intervallo chiuso* di origine a e di estremo b l'insieme dei numeri naturali che soddisfano alla $a \leq x \leq b$. Lo si denota con $[a, b]$.

Dunque, $[a, b] = \{x: x \in \mathbb{N} \text{ e } a \leq x \leq b\}$.

Sia $a < b$. Si dice *intervallo semiaperto a destra* $[a, b[$ l'insieme degli $x \in \mathbb{N}$ tali che $a \leq x < b$.

Si dice *intervallo semiaperto a sinistra* $]a, b]$ l'insieme degli $x \in \mathbb{N}$ tali che $a < x \leq b$.

Intervallo aperto $]a, b[$ è l'insieme degli $x \in \mathbb{N}$ tali che $a < x < b$.

Se $a = b$, l'intervallo chiuso contiene il solo a . Se $b = a + 1$ l'intervallo aperto è vuoto.

Fissiamo un numero naturale a . Consideriamo la funzione, definita per ogni $x \in \mathbb{N}$, $f(x) = x + a$. La funzione applica $\mathbb{N}$ sull'insieme $\mathbb{N}_a$ dei numeri naturali y tali che $y \geq a$. Ogni $y \geq a$ è l'immagine di un unico $x \in \mathbb{N}$: $x = y - a$. La funzione applica, dunque, biunivocamente $\mathbb{N}$ su $\mathbb{N}_a$. In particolare, la funzione applica biunivocamente l'intervallo $[b, c]$ sull'intervallo $[a + b, a + c]$.

APPLICAZIONI, SUCCESSIONI, EQUIPOTENZA

Abbiamo dato la seguente definizione di *applicazione*:

dati un insieme E ed un insieme F , è detta applicazione di E in F ogni legge f che associ ad ogni elemento di E un determinato elemento di F .

Se x è un elemento di E , l'elemento di F che la f gli associa si indica con $f(x)$ e si dice che $f(x)$ è l'*immagine*, oppure il *corrispondente*, di x tramite la f . E ed F si dicono rispettivamente il *dominio* ed il *codominio* della f . Se F è un insieme di numeri, le applicazioni vengono dette anche *funzioni* ed $f(x)$ si chiama il *valore* della f in x .

Per ogni sottoinsieme A di E , si indica con $f(A)$ l'insieme delle immagini degli elementi di A . Tale insieme è anche detto *insieme-immagine* di A . È: $f(A) = \{f(x) : x \in A\}$. $f(A)$ è vuoto se e solo se è vuoto A .

L'insieme $f(E)$ è detto l'*immagine* della f . Se è costituito da un solo elemento, la f si dice costante. In generale, mentre è presupposta per le applicazioni la univocità, non è invece richiesta la biunivocità, né è richiesto che $F = f(E)$.

Se è $f(E) = F$, cioè se ogni elemento di F è immagine di un elemento di E tramite la f , l'applicazione f è detta *suriettiva*. Si dice anche che la f è un'*applicazione di E su F* .

Se $\forall x_1, x_2 \in E$ è: $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$, la f è detta iniettiva. Un'applicazione, che è suriettiva e iniettiva, è detta *biettiva*.

Si conviene che, se $E = \emptyset$ e quale che sia F , esiste una applicazione di E in F , che si dice *applicazione vuota* di E in F .

Date due applicazioni f e g , tali che il codominio della f coincida col dominio della g : $f: E \rightarrow F$, $g: F \rightarrow G$, si può dedurre un'applicazione di E in G associando ad ogni $x \in E$ l'elemento $g(f(x))$ di G . Tale applicazione si dice la *composta mediante le f e g* , e si indica con $g \circ f$ o anche gf .

Qualora gf e fg esistano entrambe essendo $E=G$, in generale non sono uguali (due applicazioni sono uguali se avendo stessi dominio e codominio, qualunque sia x appartenente al dominio e supposte f, g tali applicazioni è: $f(x)=g(x)$). Lo si può verificare considerando ad esempio le due funzioni $f: \mathbb{N} \rightarrow \mathbb{N}$ definita da $f(x)=x^2$ e $g: \mathbb{N} \rightarrow \mathbb{N}$ definita da $g(x)=x+2$.

Supposto $E=F$, l'applicazione i_E definita da $i_E(x)=x$ per ogni x , è detta l'*applicazione identica* di E . Quali che siano E ed F , per ogni $f: E \rightarrow F$ è: $f i_E = i_F f = f$.

La composizione di applicazioni ha carattere associativo, cioè, se $f: E \rightarrow F$, $g: F \rightarrow G$, $h: G \rightarrow H$, è:

$$h(gf) = (hg)f.$$

Ogni applicazione si può pensare ottenuta componendo un'applicazione suriettiva con una iniettiva. Se

$f:E \rightarrow F$ e, con ovvio significato di $k, j, k:E \rightarrow f(E), j:f(E) \rightarrow F$, è: $f=jk$.

Sia $f:E \rightarrow F$ un'applicazione biettiva. Per ogni $y \in F$ esiste un elemento $x \in E$ ed uno solo che ha y come immagine. Allora, associando ad ogni y un tale x , si ha una applicazione di F in E . Tale applicazione si chiama *applicazione inversa* della f e la si indica con f^{-1} .

È: $f^{-1}(y)=x \Leftrightarrow f(x)=y$. $\forall x \in E$ è $f^{-1}(f(x))=x$, e $\forall y \in F$ è $f(f^{-1}(y))=y$, cioè: $f^{-1}f=i_E$, $ff^{-1}=i_F$. Essendo la f biettiva, lo è anche la f^{-1} e quindi ammette inversa.

Se f e g sono biettive e componibili, lo sono anche g^{-1} e f^{-1} ed è: $(fg)^{-1}=g^{-1}f^{-1}$.

Dato un insieme E , si chiama *successione* un'applicazione di N in E . Si usa, per motivi di comodità, indicare il valore della successione per un $n \in N$ con x_n , indicando x un generico elemento di E , invece che con $f(n)$. La successione stessa viene indicata con (x_n) o, per maggior precisione, con $(x_n)_{n \in N}$.

Per ricordare che E è l'insieme in cui la successione prende i suoi valori, si dice anche "*successione in E* " o "*successione di elementi di E* " o "*successione di E* ". Il valore x_n si chiama anche *termine di posto n* o *di indice n* . Un'altra notazione, che mette in evidenza in alcuni casi i valori, è: $(x_1, x_2, \dots, x_n, \dots)$.

Sia (x_n) una successione di E data. Sia d'altra parte una applicazione crescente in senso stretto di N in N , cioè una successione di interi (n_k) tale che se $k < k'$ allora

$n_k < n_{k'}$. La successione $(y_k)_{k \in \mathbb{N}}$ definita da $y_k = x_{n_k}$, per ogni k , si dice estratta dalla successione (x_n) .

Si chiama *successione doppia sopra E* un'applicazione di $\mathbb{N} \times \mathbb{N}$ in E , e la si indica con $(x_{p,q})_{(p,q) \in \mathbb{N} \times \mathbb{N}}$.

Si chiama *successione finita di E* un'applicazione di una parte finita di $\mathbb{N}$ in E .

Sia $(x_1, x_2, \dots, x_n, \dots)$ una successione tale che $\forall n, m \in \mathbb{N}$ e $n \neq m \Rightarrow x_n \neq x_m$. Una tale successione si chiama anche *progressione*. Interpretando le tre idee primitive degli assiomi di Peano come segue: "zero" significhi x_0 , "numero" significhi termine della successione, "successivo di un numero" significhi il termine successivo nella successione, cioè successivo di x_n significhi x_{n+1} , si verifica allora facilmente che i termini di una progressione verificano gli assiomi di Peano. Viceversa, si può dimostrare che una successione che verifica gli assiomi di Peano è una progressione.

Due insiemi si dicono *equipotenti* quando sono in corrispondenza biunivoca. Indicheremo che A e B sono equipotenti scrivendo $A \leftrightarrow B$.

L'equipotenza è una relazione d'equivalenza. È infatti riflessiva: $A \leftrightarrow A$; basti considerare la $i_A: A \rightarrow A$. È simmetrica: $A \leftrightarrow B \Rightarrow B \leftrightarrow A$; se $f: A \rightarrow B$ è biettiva, lo è anche $f^{-1}: B \rightarrow A$. È transitiva: $A \leftrightarrow B$ e $B \leftrightarrow C \Rightarrow A \leftrightarrow C$. La dimostrazione di tale proprietà discende dalla seguente asserzione che dimostreremo:

l'applicazione composta di due applicazioni biettive è biettiva.

Siano $f:E \rightarrow F$ e $g:F \rightarrow G$ applicazioni biettive. È $z=(gf)(x)$. Poiché g è biettiva, è $F \leftrightarrow G$ e z è l'immagine di un unico $y \in E$ nell'applicazione composta gf .

Si dice che un insieme A è finito se è equipotente ad un intervallo $[1, n]$ di N . Il numero n si chiama il *numero cardinale* dell'insieme A . L'insieme vuoto ha cardinale 0.

Affinché due insiemi finiti siano equipotenti, è necessario e sufficiente che essi abbiano lo stesso numero cardinale.

Siano A, B due insiemi tali che $A \leftrightarrow B$ e sia n il numero cardinale di A , cioè $A \leftrightarrow [1, n]$. Per la simmetria e la transitività dell'equipotenza è: $B \leftrightarrow A$ e $A \leftrightarrow [1, n] \Rightarrow B \leftrightarrow [1, n]$, cioè n è anche cardinale di B .

Viceversa, se A e B hanno lo stesso cardinale n , cioè $A \leftrightarrow [1, n]$ e $B \leftrightarrow [1, n]$, per la simmetria e la transitività della relazione di equipotenza è:

$$A \leftrightarrow [1, n] \text{ e } [1, n] \leftrightarrow B \Rightarrow A \leftrightarrow B.$$

Si dimostra che:

il cardinale della riunione di due insiemi finiti disgiunti è uguale alla somma dei cardinali di questi insiemi.

Conseguenze di questo teorema sono:

- a) ogni parte P di un insieme finito A possiede un cardinale non superiore a quello di A ;
- b) ogni parte P di un insieme finito A e distinta da A possiede un cardinale strettamente inferiore a quello di A .

Dimostriamo la proposizione a). Se $P' = {}_{C_A}P$ è $A = P \cup P'$ e $P \cap P' = \emptyset$. Pertanto, se a, p, p' sono i cardinali rispettivamente di A , di P e di P' , è: $a = p + p' \Rightarrow a \geq p$.

Dimostriamo la proposizione b).

È: $P \neq A \Rightarrow P' = {}_{C_A}P \neq \emptyset$, per cui $p' \neq 0$. È: $a = p + p'$ e $p' \neq 0 \Rightarrow a > p$.

Si chiama insieme *infinito* un insieme che non è finito. Se un insieme E è equipotente ad una parte propria di A , cioè $A \subset E$ e $A \neq E$, allora è infinito. Supponiamo E finito e dimostriamo che si perviene ad una contraddizione. $A \leftrightarrow E \Rightarrow$ cardinale di $A =$ cardinale di E ; d'altra parte: $A \subset E$ e $A \neq E \Rightarrow$ cardinale di $A <$ cardinale di E . Dunque E non può essere finito.

Si dice che un insieme E è *infinito numerabile*, o semplicemente *numerabile*, se è equipotente all'insieme N dei numeri naturali.

Nella corrispondenza $E \leftrightarrow N$ ad ogni $n \in N$ corrisponde un elemento $a \in E$ che si indica con a_n . L'ordine totale in N è allora indotto in E .

Nell'insieme N , per un $x \in N$ qualsiasi si ha $x \geq 0$. 0 si chiama l'elemento *più piccolo* o il *minimo* di N .

Consideriamo una parte A di N . Se esiste un elemento $a \in A$ tale che $x \geq a$ per qualsiasi $x \in A$, a si chiama allora l'elemento *più piccolo* o il *minimo* della parte A . Se il minimo $a \in A$ esiste, allora è unico. Difatti, se esistesse un altro elemento minimo a' , sarebbe $a \geq a'$ e $a' \geq a$, cioè $a' = a$.

Se esiste un elemento $b \in A$ tale che $x \leq b$ per un qualsiasi $x \in A$, allora b si chiama l'elemento *più grande* o

il massimo di A . Se un tale b esiste, esso è unico. N non possiede un elemento più grande poiché per un $a \in N$ qualsiasi esiste un $x \in N$ tale che $x > a$, per esempio $x = a + 1$.

Dimostriamo che: *ogni parte finita A non vuota di N ammette un elemento più grande ed un elemento più piccolo.*

Per $n=1$ il teorema è banale. Per $n=2$, è $A = \{a, b\}$ e poiché l'ordine in N è totale, sappiamo confrontare a e b e dire quale è il più grande (rispettivamente il più piccolo). Supponiamo di aver dimostrato la proposizione: "*ogni parte A di cardinale $n-1$ ammette un elemento più grande*" e proviamo che "*ogni parte di A di cardinale n ammette un elemento più grande*". Si può considerare qualsiasi parte A di n numeri naturali come l'unione di una parte A' di $n-1$ numeri naturali e di un insieme con un unico elemento a : $A = A' \cup \{a\}$. Per l'ipotesi di ricorrenza possiamo dire che A' ammette un elemento più grande b . L'insieme $\{a, b\}$ ammette un elemento più grande che è l'elemento più grande di A .

Lo stesso per l'elemento minimo.

Dimostriamo che: *se una parte non vuota di N ammette un elemento più grande, essa è finita.*

Sia A una parte non vuota di N con un elemento più grande a . $x \in A \Rightarrow x \leq a$ ($a \in A$), A è quindi incluso nell'intervallo $[0, a]$ che è finito, ed una parte A di un insieme finito $[0, a]$ è essa stessa finita.

Concludendo:

condizione necessaria e sufficiente perché una parte non vuota di N abbia un elemento più grande, è che essa sia finita.

Ne segue che: *ogni parte infinita di N non ammette un massimo.*

Dimostriamo che: *ogni parte infinita P di N ammette un elemento più piccolo.*

Sia $a \in P$: se esistono in P degli elementi inferiori ad a , essi appartengono all'intervallo $[0, a]$ e costituiscono l'intersezione $J = P \cap [0, a]$. J non è vuoto, poiché contiene almeno a ; J è finito poiché è incluso in $[0, a]$, dunque J ammette un elemento più piccolo che è l'elemento più piccolo di P .

Sia A una parte di N . Se esiste un numero $a \in N$ tale che $x \leq a$ per un qualsiasi $x \in A$, si dice che a è un *maggiorante* di A o che a *maggiora* A o che A è *maggiorato* da a . Se esiste un numero $b \in N$ tale che $x \geq b$ per un qualsiasi $x \in A$, si dice che b è un *minorante* di A , o che b *minora* A oppure che A è *minorato* da b . Se A è maggiorato da a , qualsiasi numero superiore ad a è anch'esso un maggiorante di A . Se A è minorato da b , qualsiasi numero inferiore a b è anch'esso un minorante di A .

Dimostriamo che: *ogni parte maggiorata di N è finita.* Infatti, se la parte A di N è maggiorata da a , essa è inclusa in $[0, a]$ ed è per conseguenza finita.

POTENZA DEL NUMERABILE

Consideriamo l'insieme $\mathbf{N}$ dei numeri naturali e consideriamo $\mathbf{N} \cup \{\mathbf{s}\}$ dove $\mathbf{s} \notin \mathbf{N}$. Fra $\mathbf{N} \cup \{\mathbf{s}\}$ ed $\mathbf{N}$ si può ottenere una corrispondenza biunivoca come segue:

$\mathbf{N} \cup \{\mathbf{s}\}$		$\mathbf{N}$
$\mathbf{s}$	$\leftrightarrow$	0
0	$\leftrightarrow$	1
1	$\leftrightarrow$	2
.....		
.....		
$\mathbf{n}$	$\leftrightarrow$	$\mathbf{n}+1$
.....		
.....		

Dunque $\mathbf{N} \cup \{\mathbf{s}\} \leftrightarrow \mathbf{N}$, e indicando con $|\mathbf{N}|$ il cardinale di $\mathbf{N}$ è: $|\mathbf{N}|+1=|\mathbf{N}|$. Poiché se $\mathbf{a}$ è un cardinale finito, $\mathbf{a}+1 \neq \mathbf{a}$, $|\mathbf{N}|$ non è uguale ad alcun cardinale finito. Il cardinale dell'insieme $\mathbf{N}$ è un cardinale *transfinito* e viene denotato con $\aleph_0$ (aleph-zero).

Ogni sottoinsieme infinito di un insieme numerabile è numerabile. Sia $\mathbf{A}$ un insieme numerabile. I suoi elementi possono essere ordinati in successione: $\mathbf{A}=\{\mathbf{a}_0, \mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_r, \dots, \mathbf{a}_s, \dots\}$. Se $\mathbf{B}$ è un sottoinsieme di $\mathbf{A}$, ogni elemento di $\mathbf{B}$ è anche elemento di $\mathbf{A}$. Supponiamo

che sia $\mathbf{B}=\{\mathbf{a}_p, \mathbf{a}_q, \mathbf{a}_r, \mathbf{a}_s, \dots\}$. Se $\mathbf{B}$ è infinito, l'insieme $\mathbf{I}$ degli indici, $\mathbf{I}=\{\mathbf{p}, \mathbf{q}, \mathbf{r}, \mathbf{s}, \dots\}$, è un sottoinsieme infinito di $\mathbf{N}$. Esso possiede un primo elemento: se questo è $\mathbf{p}$, poniamo $\mathbf{a}_p=\mathbf{b}_0$. Il complemento di $\{\mathbf{p}\}$ in $\mathbf{I}$ è anch'esso un sottoinsieme di $\mathbf{N}$ e quindi possiede un primo elemento: se questo è $\mathbf{q}$, poniamo $\mathbf{a}_q=\mathbf{b}_1$. Per la stessa ragione il complemento di $\{\mathbf{p}, \mathbf{q}\}$ in $\mathbf{I}$ possiede un primo elemento. Se questo è $\mathbf{r}$, poniamo $\mathbf{a}_r=\mathbf{b}_2$ e così via. Essendo $\mathbf{B}$ infinito per ipotesi, questo procedimento non ha termine e rende anche possibile l'ordinamento degli elementi di $\mathbf{B}$ in successione. $\mathbf{B}=\{\mathbf{b}_0, \mathbf{b}_1, \mathbf{b}_2, \dots\}$. Dunque $\mathbf{B}$ è equipotente ad $\mathbf{N}$ e quindi è numerabile.

Dimostriamo che non esiste alcun insieme infinito di potenza inferiore alla potenza del numerabile. Sia $\mathbf{A}$ un insieme infinito. Supponiamo che $|\mathbf{A}| < \aleph_0$, ciò significa che esiste $\mathbf{N}' \subset \mathbf{N}$ per cui $\mathbf{A} \leftrightarrow \mathbf{N}' \subset \mathbf{N}$ e non esiste un $\mathbf{A}' \subset \mathbf{A}$ per cui $\mathbf{N} \leftrightarrow \mathbf{A}' \subset \mathbf{A}$. $\mathbf{A}$ infinito $\Rightarrow \mathbf{N}'$ infinito, ma essendo $\mathbf{N}' \subset \mathbf{N}$ e infinito, per il teorema precedente $\mathbf{N}'$ è numerabile per cui $|\mathbf{A}| = \aleph_0$, che contraddice l'ipotesi.

Dimostriamo che per ogni $\mathbf{n}$ cardinale finito è $\aleph_0 + \mathbf{n} = \aleph_0$.

Consideriamo l'intervallo $[0, \mathbf{n}-1]$ di cardinale $\mathbf{n}$ e sia $\mathbf{N}'$ il suo complemento in $\mathbf{N}$. È $[0, \mathbf{n}-1] \cup \mathbf{N}' = \mathbf{N}$. Ma $\mathbf{N}'$ è equipotente con $\mathbf{N}$, quindi è $\aleph_0 + \mathbf{n} = \aleph_0$.

Dimostriamo che $\aleph_0 + \aleph_0 = \aleph_0$.

L'insieme $\mathbf{A}=\{\mathbf{a}_0, \mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3, \dots\}$ può essere considerato come $\mathbf{A}=\{\mathbf{a}_0, \mathbf{a}_2, \mathbf{a}_4, \dots\} \cup \{\mathbf{a}_1, \mathbf{a}_3, \mathbf{a}_5, \dots\}$. Entrambi hanno la potenza del numerabile.

Si dimostra anche che $n \cdot \aleph_0 = \aleph_0$ e $\aleph_0 \cdot \aleph_0 = \aleph_0$.

Si dimostrano le seguenti proposizioni:

- L'insieme $\mathbf{Z}$ degli interi relativi è numerabile.
- L'insieme $\mathbf{Q}$ dei razionali è numerabile.

Insieme delle parti di un insieme E è l'insieme che ha per elementi i sottoinsiemi di E . Esso viene indicato con $\mathcal{P}(E)$. Si dimostra che: *l'insieme delle parti di un qualunque insieme A ha potenza superiore alla potenza di A* . Si dimostra anche che l'insieme delle parti di un insieme numerabile ha potenza superiore al numerabile. Tale potenza si dice *potenza del continuo*.

L'insieme dei numeri reali ha la potenza del continuo. L'insieme dei punti di un segmento ha la potenza del continuo. L'insieme dei punti di un quadrato è equipotente all'insieme dei punti di un suo lato. L'insieme dei punti di un cubo è equipotente all'insieme dei punti di un suo spigolo.

IL PRODOTTO IN $\mathbf{N}$

Ad ogni coppia ordinata $(\mathbf{x}, \mathbf{y})$ di numeri naturali facciamo corrispondere un numero naturale, detto prodotto di $\mathbf{x}$ per $\mathbf{y}$ ed indicato con $\mathbf{xy}$ o $\mathbf{x} \cdot \mathbf{y}$, e definito per ricorrenza come segue:

- a) $\mathbf{x} \cdot \mathbf{0} = \mathbf{0}$
- b) supposto $\mathbf{xy}$ definito, si definisce $\mathbf{xy}^+$ come:
 $\mathbf{xy}^+ = \mathbf{xy} + \mathbf{x}$.

Cerchiamo l'insieme $\mathbf{A}$ dei numeri naturali $\mathbf{y}$, per i quali, fissato $\mathbf{x}$, la moltiplicazione risulta definita.

Innanzitutto $\mathbf{0} \in \mathbf{A}$ poiché a) definisce l'operazione per $\mathbf{y} = \mathbf{0}$. Supponendo la moltiplicazione definita per $\mathbf{y}$, assumendo cioè $\mathbf{xy}$ definito, la b) definisce $\mathbf{xy}^+$, pertanto è $\mathbf{y} \in \mathbf{A} \Rightarrow \mathbf{y}^+ \in \mathbf{A}$. Per l'assioma (A5) allora $\mathbf{A} = \mathbf{N}$, cioè è definita per tutti i numeri naturali.

Applicando la b) per $\mathbf{y} = \mathbf{0}$ è: $\mathbf{x} \cdot \mathbf{0}^+ = \mathbf{x} \cdot \mathbf{0} + \mathbf{x}$, ed essendo $\mathbf{0}^+ = \mathbf{1}$ e $\mathbf{x} \cdot \mathbf{0} = \mathbf{0}$ si ha: $\mathbf{x} \cdot \mathbf{1} = \mathbf{x}$.

Valgono le seguenti proprietà:

$\forall \mathbf{x}, \mathbf{y}, \mathbf{z}$ è: $\mathbf{x}(\mathbf{y} + \mathbf{z}) = \mathbf{xy} + \mathbf{xz}$ (*distributività della moltiplicazione rispetto all'addizione*)

$\forall \mathbf{x}, \mathbf{y}, \mathbf{z}$, se $\mathbf{y} \geq \mathbf{z}$ allora $\mathbf{x}(\mathbf{y} - \mathbf{z}) = \mathbf{xy} - \mathbf{xz}$ (*distributività della moltiplicazione rispetto alla sottrazione*)

$\forall \mathbf{x}, \mathbf{y}, \mathbf{z}$ è: $(\mathbf{xy})\mathbf{z} = \mathbf{x}(\mathbf{yz})$ (*associatività*)

$\forall \mathbf{x}, \mathbf{y}$ è: $\mathbf{xy} = \mathbf{yx}$ (*commutatività*).

In particolare è $x \cdot 1 = 1 \cdot x = x$, cioè **1** è l'*elemento neutro* per la moltiplicazione.

Dimostriamo che: *se un prodotto di due numeri è nullo, almeno uno di questi numeri è nullo.*

Sia $ab=0$ e dimostriamo che almeno uno dei due numeri **a** e **b** è zero. Se nessuno dei due fosse zero, esisterebbero a' e b' tali che $a=a'+1$, $b=b'+1$, per cui:

$$0=ab=(a'+1)(b'+1)=a'b'+a'+b'+1,$$

ma questo contraddice l'assioma (A3), dunque **a** e **b** non possono entrambi essere diversi da zero.

Dati **a**, **b** numeri naturali, $\forall x \in \mathbf{N}$, $x \neq 0$ è $ax=bx \Rightarrow a=b$.

È: $ax=bx \Rightarrow ax-bx=0 \Rightarrow (a-b)x=0$ e, poiché $x \neq 0$, ne consegue $a-b=0 \Rightarrow a=b$.

Questa proprietà si esprime dicendo che ogni numero naturale diverso da zero è *semplificabile* o *regolare* per la moltiplicazione.

Se **a**, **b** sono naturali, $ab=1 \Rightarrow a=b=1$.

Siano **a**, **b** tali che $ab=1$. Né **a** né **b** possono essere zero perché sarebbe $ab=0$. Pertanto esistono a' e b' tali che $a=a'+1$ e $b=b'+1$. È: $1=ab=(a'+1)(b'+1)=a'b'+a'+b'+1$, da cui è: $0=a'b'+a'+b'$ e $a'=b'=a'b'=0$. Pertanto $a=1$ e $b=1$.

Per quanto riguarda la moltiplicazione e la relazione d'ordine si dimostrano le proposizioni seguenti.

Siano **a**, **b** numeri naturali:

$$\forall c \in \mathbf{N}, a \leq b \Rightarrow ac \leq bc$$

$$\forall c \in \mathbf{N} \text{ e } c \neq 0, a < b \Leftrightarrow ac < bc.$$

Siano a, b, c, d numeri naturali:

$$a \leq b \text{ e } c \leq d \Rightarrow ac \leq bd$$

$$a < b \text{ e } c < d \Rightarrow ac < bd.$$

Sia a un numero naturale diverso da 0 . Ad ogni numero naturale x facciamo corrispondere un numero naturale indicato con a^x e definito per ricorrenza come segue:

$$a) \quad a^0 = 1$$

$$b) \quad \text{supposto } a^x \text{ definito definiamo } a^{x+} \text{ come:} \\ a^{x+} = ax \cdot a.$$

È definita così per ricorrenza in $\mathbf{N}$ la funzione a^x di x con immagini in $\mathbf{N}$ che è detta “*potenza di esponente x di a* ”. Se $a=1$, tutti i numeri $x \in \mathbf{N}$ hanno la stessa immagine.

Valgono le seguenti proprietà:

$$a^x \cdot a^y = a^{x+y}$$

$$(a^x)^y = a^{xy}$$

$$a^x b^x = (ab)^x.$$

Siano a, b numeri naturali, $\forall x \in \mathbf{N}$ e $x \neq 0$, $a < b \Leftrightarrow a^x < b^x$. Supposto $x \neq 0$ dimostriamo $a < b \Rightarrow a^x < b^x$. L'implicazione è vera per $x=1$. Supponiamo di aver stabilito che $a < b \Rightarrow a^x < b^x$, dimostriamo che $a < b \Rightarrow a^{x+} < b^{x+}$. Per l'ipotesi di ricorrenza è vera $a < b$ e $a^x < b^x$. Moltiplicando membro a membro si ha $a^{x+} < b^{x+}$. Dimostriamo ora che $a^x < b^x \Rightarrow a < b$. Supposto $a \geq b$, seguirebbe $a^x \geq b^x$ in contraddizione con l'ipotesi. Pertanto $a < b$.

$$a > 1 \text{ e } x > y \Rightarrow a^x > a^y.$$

È: $x > y \Rightarrow \exists d \neq 0: x = y + d; a > 1 \text{ e } d \neq 0 \Rightarrow a^d > 1$. Moltiplicando i due membri per a^y che non è nullo, si ha: $a^y \cdot a^d > a^y$, cioè $a^{y+d} > a^y$ e dunque $a^x > a^y$.

L'immagine di $\mathbf{N}$ per la funzione a^x è una parte di $\mathbf{N}$, che indichiamo con P_a e si chiama "*progressione geometrica di primo elemento 1 e ragione a*":

$$P_a = \{1, a, a^2, a^3, \dots, a^x, \dots\}$$

Siano E ed F due insiemi ordinati con relazioni che indicheremo entrambe con $<$. Si dice che una funzione f , definita in E con valori in F , è *crescente* se $x < y \Rightarrow f(x) < f(y)$.

Si dice che f è *decrecente* se $x < y \Rightarrow f(x) > f(y)$.

La funzione a^x è crescente in quanto è $x > y \Rightarrow a^x > a^y$.

Proviamo che: $a > 1 \text{ e } a^x = a^y \Rightarrow x = y$.

Se si supponesse $x > y$ si avrebbe $a^x > a^y$ in contraddizione con l'ipotesi e lo stesso se si supponesse $x < y$, pertanto $x = y$. La funzione a^x dunque applica biunivocamente $\mathbf{N}$ su P_a ($a > 1$). La funzione inversa di $y = a^x$ si chiama *logaritmo in base a* e si indica con $x = \lg_a y$. Essa è definita per $y \in P_a$ ed applica P_a su $\mathbf{N}$.

Si dimostra la seguente proprietà fondamentale:

$$\forall y', y'' \in P_a \text{ è: } \lg_a y' + \lg_a y'' = \lg_a (y' y'').$$

Dato un numero a , consideriamo la funzione definita in $\mathbf{N}$ da: $f(x) = ax$. $f(x)$ si chiama *multiplo* di a . Indicheremo con M_a l'insieme immagine $f(\mathbf{N})$.

È:

$$a=0 \Rightarrow f(x)=0 \quad \forall x \in \mathbf{N} \Rightarrow M_a=\{0\}$$

$$a=1 \Rightarrow f(x)=x \quad \forall x \in \mathbf{N} \Rightarrow M_a=\mathbf{N}$$

$$a=2 \Rightarrow f(x)=2x \Rightarrow M_a \text{ è l'insieme dei numeri pari.}$$

Per $a \neq 0$ è $M_a=\{0, a, 2a, \dots, ka, \dots\}$.

Se $a \neq 0$ la funzione $f(x)=ax$ è crescente. È $a \neq 0$ e $x' < x'' \Rightarrow ax' < ax''$.

Vale anche il reciproco: $a \neq 0$ e $ax' < ax'' \Rightarrow x' < x''$.

Si ha anche che: $y' \geq y''$ e $y', y'' \in M_a \Rightarrow y' + y'' \in M_a$ e $y' - y'' \in M_a$ e $y'y'' \in M_a$, come facilmente si dimostra.

Se $a \neq 0$, ad ogni $y \in M_a$ corrisponde un solo $x \in \mathbf{N}$ tale che $y=ax$. Infatti $ax'=ax''$ e $a \neq 0 \Rightarrow x'=x''$. Questa proprietà dimostra che la funzione $f(x)=ax$ applica biunivocamente $\mathbf{N}$ su M_a per $a \neq 0$. La funzione inversa, che applica M_a su $\mathbf{N}$, viene indicata simbolicamente con $f^{-1}(y) = \frac{y}{a}$.

Da quanto detto il simbolo $\frac{y}{a}$ vale solo se y è un multiplo di a ; si dice allora che a divide y e si scrive $a | y$. Si dice anche che " a è un divisore di y " o che " y è divisibile per a ". Il numero x controimmagine di y nella f si chiama "quoziente esatto di y per a ".

Dati due numeri a e b ($b \neq 0$), esiste uno ed un solo intero q tale che: $bq \leq a < b(q+1)$.

Siano a, b ($b \neq 0$), consideriamo $M_b=\{0, b, 2b, \dots, nb, \dots\}$. Sia P : $x \in P \Leftrightarrow x \in M_b$ e $x \leq a$. P è l'insieme dei multipli di b al più uguali ad a . P non è vuoto perché contiene almeno lo 0. È finito perché è maggiorato da a . Ammette perciò un mas-

simo $\mathbf{m}$ che è dunque il più grande multiplo di $\mathbf{b}$ al più uguale ad $\mathbf{a}$. Poiché $\mathbf{m} \in \mathbf{M}_b$ esiste un intero $\mathbf{q}$, che è unico perché $\mathbf{b} \neq 0$, tale che $\mathbf{m} = \mathbf{bq}$. È evidentemente $\mathbf{bq} \leq \mathbf{a}$.

Dimostriamo che anche $(\mathbf{q}+1)\mathbf{b} > \mathbf{a}$. Se fosse $(\mathbf{q}+1)\mathbf{b} \leq \mathbf{a}$ si avrebbe $(\mathbf{q}+1)\mathbf{b} \in \mathbf{P}$, con $(\mathbf{q}+1)\mathbf{b} = \mathbf{qb} + \mathbf{b} > \mathbf{qb}$ perché $\mathbf{b} \neq 0$, e dunque $\mathbf{qb}$ non sarebbe il massimo di $\mathbf{P}$.

Determinare l'intero $\mathbf{q}$ significa effettuare la *divisione euclidea* di $\mathbf{a}$ per $\mathbf{b}$. $\mathbf{a}$ si chiama *dividendo*, $\mathbf{b}$ *divisore* e $\mathbf{q}$ *quoziente euclideo*.

Dimostriamo che:

$$\mathbf{bq} \leq \mathbf{a} < \mathbf{b}(\mathbf{q}+1) \Leftrightarrow \exists \mathbf{r}: \mathbf{a} = \mathbf{bq} + \mathbf{r} \text{ e } \mathbf{r} < \mathbf{b}.$$

Si ha:

$$\mathbf{bq} \leq \mathbf{a} \Rightarrow \exists \mathbf{r} \text{ unico: } \mathbf{a} = \mathbf{bq} + \mathbf{r}; \mathbf{a} < \mathbf{b}(\mathbf{q}+1) \Rightarrow \mathbf{bq} + \mathbf{r} < \mathbf{bq} + \mathbf{b} \Rightarrow \mathbf{r} < \mathbf{b}.$$

Viceversa, se esistono $\mathbf{q}$ ed $\mathbf{r}$ tali che $\mathbf{a} = \mathbf{bq} + \mathbf{r}$ e $\mathbf{r} < \mathbf{b}$, si ha: $\mathbf{a} = \mathbf{bq} + \mathbf{r} \Rightarrow \mathbf{a} \geq \mathbf{bq}$, $\mathbf{r} < \mathbf{b} \Rightarrow \mathbf{bq} + \mathbf{r} < \mathbf{bq} + \mathbf{b} \Rightarrow \mathbf{a} < \mathbf{b}(\mathbf{q}+1)$.

Il numero $\mathbf{r}$ si chiama il *resto* della divisione euclidea di $\mathbf{a}$ per $\mathbf{b}$. Se $\mathbf{b} \mid \mathbf{a}$ è $\mathbf{a} = \mathbf{bq}$ e di conseguenza $\mathbf{r} = 0$. Reciprocamente, se $\mathbf{r} = 0$, $\mathbf{a} = \mathbf{bq}$ perciò $\mathbf{b} \mid \mathbf{a}$. Pertanto: *condizione necessaria e sufficiente perché $\mathbf{b}$ divida $\mathbf{a}$ è che il resto della divisione euclidea di $\mathbf{a}$ per $\mathbf{b}$ sia nullo.*

Il quoziente euclideo ha le seguenti proprietà di facile dimostrazione.

Se $\mathbf{q}$ è il quoziente euclideo di $\mathbf{a}$ per $\mathbf{b}$ e se $\mathbf{q}'$ è il quoziente euclideo di $\mathbf{q}$ per $\mathbf{c}$, $\mathbf{q}'$ è anche il quoziente euclideo di $\mathbf{a}$ per $\mathbf{bc}$.

Se q e q' sono i quozienti euclidei rispettivamente di a ed a' per b , si ha: $a' \geq a \Rightarrow q' \geq q$.

Se q e q' sono i quozienti euclidei rispettivamente di a per b e b' , si ha: $b' \geq b \Rightarrow q' \leq q$.

INDICE

Premesse insiemistiche	5
I numeri naturali	9
La relazione d'ordine totale in $\mathbb{N}$	14
Applicazioni, successioni, equipotenza	18
Potenza del numerabile.....	26
Il prodotto in $\mathbb{N}$	29

Notizia

Sergio Fumich è nato a Trieste nel 1947. Dal 1970 si è trasferito a Brembio, piccolo comune del Lodigiano. Lavora a Milano presso un'importante Fondazione lombarda che si occupa di formazione professionale. Ha svolto attività pubblicistica dal 1978 al 1995 come collaboratore del quotidiano di Lodi *Il Cittadino*, come direttore responsabile di alcuni fogli locali e della rivista di poesia *Keraunia*. Ha pubblicato libri di poesia e di racconti e opuscoli divulgativi.

Ca' "La Gatera"

Edizione fuori commercio

Finito di stampare a Brembio (LO) con tecniche elettroniche nel novembre 2005

Di questo opuscolo sono stati tirati 200 esemplari.

